IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. HAILONG ZHU, Defendant.	**UNDER SEAL** Case No. 1:23-MJ-63

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Christopher L. Saunders, being duly sworn, depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent employed by the U.S. Secret Service (USSS). I have been employed as a Special Agent with the USSS since 2018, and I am currently assigned to the Criminal Investigative Division. Upon entering the USSS, I completed 18 weeks of basic training. This training covered various aspects of federal law enforcement, including instruction on how to investigate financial crimes. I am a Certified Public Accountant (CPA) and have investigated numerous individuals for a wide variety of federal and state felony offenses, including wire fraud, bank fraud, computer intrusion, and access device fraud. Furthermore, I have attended more than 120 hours of USSS training pertaining to cyber and electronic crimes.

2. This affidavit is submitted in support of a criminal complaint and arrest warrant for HAILONG ZHU for conspiring to commit money laundering, in violation of Title 18, United States Code, Section 1956(h).

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show only that there is sufficient probable cause for the requested complaint and arrest warrant and does not set forth all of my knowledge about this matter. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, knowledge of the investigation, and reasonable inferences that I have drawn from my training, experience, and knowledge of the investigation.

TECHNICAL BACKGROUND

4. "Digital currency" or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[1] Examples of cryptocurrency are Bitcoin (or BTC) and Ether (or ETH). Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Most cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

[1] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[2] Some cryptocurrencies operate on blockchains that are not public.

5. "Bitcoin"[3] is a decentralized digital currency that can be used and transferred electronically from person-to-person independent of financial institutions. Bitcoin transactions are maintained in a ledger that can be accessed electronically from anywhere in the world. Bitcoin often is used by cybercriminals to conduct illicit transactions because of its perceived anonymity and its ability to be transferred between people anywhere in the world. Bitcoin is stored on the Bitcoin network in what are called bitcoin addresses. Bitcoin holders transmit bitcoin between bitcoin addresses. Each bitcoin address is controlled using a unique, corresponding private key — a kind of cryptographic password needed to access the address. Only the owner of the private key for an address can authorize the transfer of bitcoin from that address to another bitcoin address. Bitcoin addresses are often stored alongside their corresponding private keys in digital wallets. No identifying information about the payor or payee is transmitted in a bitcoin transaction, as generally only the bitcoin addresses of the parties are needed for the transaction.

6. A user typically acquires bitcoin from "bitcoin exchanges." Bitcoin exchanges generally accept payments of fiat currency, and, for a fee, transfer a corresponding number of bitcoin to the customer. Exchanges likewise can be used to convert bitcoin back into fiat currency.

7. Tether ("USDT") and USD Coin ("USDC") are alternative types of cryptocurrency or altcoin tokens. Payments or transfers of value made with USDT and USDC are recorded in the blockchain network, but unlike decentralized cryptocurrencies like bitcoin, USDT has some anatomical features of centralization. One centralized feature is that USDT and USDC are "stablecoins," where the value of the digital asset is pegged to a reference asset (in this case, the dollar); for each USDT and USDC issued, the tokens are represented to be backed by $1 of asset

[3] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

reserves. These characteristics make them theoretically less volatile than bitcoin, and consequently wallet holders typically hedge their cryptocurrency holdings into USDT in an attempt to protect their receipt or earnings value, so it is not affected by the rest of the volatile cryptocurrency market.

8. An "Internet Protocol address" or "IP address" is a numerical address assigned to each computer connected to a network that uses the internet for communication. Internet Service Providers assign IP addresses to their customers. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access an account. The type of application or service provider a particular customer is using often determines how long they will be assigned the same IP address. For instance, someone who rents computer servers can lease an IP address long term and maintain it for several years. In my training and experience, residential Internet Service Providers often lease the same IP address to a customer over months to a year. Cellular phone provider customer IP addresses often change more frequently due to customers being more transient. Email providers, internet providers, and even cybercrime forums often record the IP address used to register an account and the IP addresses associated with particular logins to the account. In my training and experience, when the same IP address is used to access different internet services in close temporal proximity, it tends to show the same computer or computer network was used to access those services. When several instances of this IP overlap exist over time from different service providers, it makes it very likely that the same person or group of people sharing internet infrastructure are behind the accesses.

9. A domain name is a simple, easy-to-remember way for humans to identify computers on the internet, using a series of characters (*e.g.*, letters, numbers, or other characters)

that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

10. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

PROBABLE CAUSE

A. Case Background

11. In September 2022, law enforcement began an investigation of criminal money laundering syndicates operating cryptocurrency investment scams. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S. victims. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

12. This type of scam is often called "Pig Butchering" (derived from the Chinese phrase, which is used to describe this scheme) and involves scammers spending significant time getting to know and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided bitcoin, USDT, ETH or USDC deposit address, and are further told that they can expect to make a sizable return on their investments. As investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which encourages the victim to

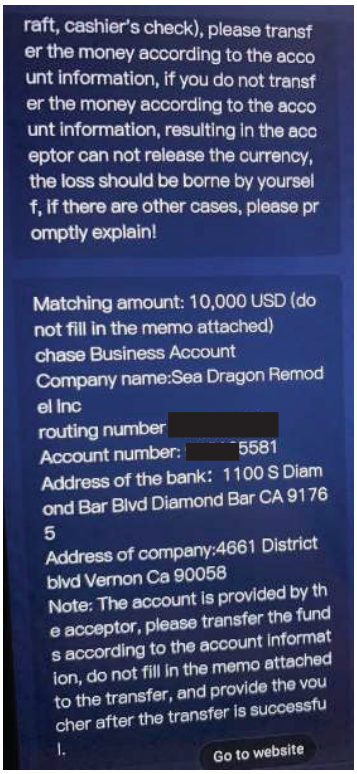
continue making investments. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve any portion of their investment.

13. As of January 20, 2023, the USSS had identified over 15 victims associated with one particular "Pig Butchering" syndicate, which has resulted in over 20 million dollars in losses. The most prolific spoofed domain within this syndicate is a fraudulent cryptocurrency investment scam involving numerous spoofed domains of the Singapore International Monetary Exchange ("SIMEX"), which has the legitimate domain name sgx.com. These spoofed domains use copyright and trademark information from legitimate cryptocurrency investment trading platforms to appear recognizable to victims. During this investigation, the USSS has interviewed various victims. Each of the victims was induced through fraud to invest, and none has been able to recover any of their losses.

14. On or about September 1, 2022, law enforcement conducted an undercover operation in which an undercover agent (hereinafter, "UCA") visited and created an account at one of the spoofed domains sent to some of the victims, simexlua.com. Law enforcement chose this domain because a number of victims were fraudulently induced to visit this domain and invest funds, which they subsequently were informed, through the simexlua.com chat portal, that they had lost. The UCA began communicating with online customer service, through the chat portal, about making investments. Shortly thereafter, online customer service provided the UCA with instructions to invest funds by sending a wire to a company named, "Sea Dragon Remodel Inc,"

as shown in Figure 1 below. The wire address was provided in an attempt to make the UCA believe the bank account was owned and operated by SIMEX. While the scammers prefer cryptocurrency deposits, they will also accept bank wires if the victim cannot transfer cryptocurrency.

Figure 1



B. HAILONG ZHU's Bank Account Activity

15. Law enforcement obtained legal process for the account displayed in Figure 1, which is a JPMorgan Chase (hereinafter, "JPMC") account. According to JPMC records, the account ending in 5581 (hereinafter, "JPMC account 5581") was opened by HAILONG ZHU (hereinafter, "ZHU") on October 21, 2022, for a business called Sea Dragon Remodel Inc. ZHU was the sole signatory listed on the account. In the documents used to open the bank account, ZHU provided a date of birth, social security number, and an address of 4661 District Blvd in Vernon, California. ZHU provided a phone number ending in 1546 ("phone number 1546"), and an email address of zhuhailong923@gmail.com. As explained below, this information — except for the

address and email address — is the same as that of the Sea Dragon Trading LLC information.

16. According to records obtained from the California Secretary of State, on October 17, 2022, ZHU filed to incorporate Sea Dragon Remodel Inc., with a listed address of 4661 District Blvd, Vernon, California. According to open-source information, a warehouse is located at this location and this address is also associated with several other companies. According to the records obtained from the California Secretary of State, ZHU is the sole agent, as well as the Chief Executive Officer, Chief Financial Officer, and Secretary. On the Statement of Information form filed with the California Secretary of State, ZHU stated that Sea Dragon Remodel would be involved in "remodel [sic] and distribution of construction material."

17. According to JPMC records, ZHU is the sole signatory of a bank account ending in 3886 (hereinafter, "JPMC account 3886"), which was opened as a business checking account on September 9, 2022, for a business called Sea Dragon Trading LLC. In the documents used to open the bank account, ZHU provided his date of birth, social security number, phone number 1546, and an email of hailong923@gmail.com. The listed address on the bank documents for Sea Dragon Trading LLC is an address located on S El Molino St in Alhambra, California.

18. According to records obtained from the California Secretary of State, on September 8, 2022, ZHU filed to incorporate Sea Dragon Trading LLC, with the same address on S El Molino St in Alhambra. ZHU is the sole registered agent for this company, as well as the Chief Executive Officer. On the statement of information filed with the California Secretary of State, ZHU stated Sea Dragon Trading LLC would be engaged in "general trading."

19. According to Bank of America records, ZHU opened a business account ending in 9529 (hereinafter, "BOA account 9529") on October 20, 2022, for a business called Sea Dragon Remodel Inc. According to the records, the listed address for this account is located on Falling

Leaf Ave in Rosemead, California.

20. Additional financial records revealed that between September 2021 and October 2022, ZHU opened at least one additional account at Bank of America, as well as accounts at U.S. National Bank and Wells Fargo both in his name and the names of his businesses (Sea Dragon Trading LLC and Sea Dragon Remodeling). Refer to **Figure 3** below for details. Further, ZHU is the only listed signatory for each of these accounts. Based on my training and experience, I know that it is not normal for a legitimate business to open so many bank accounts under the same business name and numerous addresses. Additionally, I believe that the pattern of incorporating various businesses in close succession with the California Secretary of State, and opening various bank accounts almost immediately thereafter, is consistent with the creation of shell companies used for money laundering. As further explained below, there is probable cause to support that ZHU opened these accounts and then used these accounts to launder proceeds illegally obtained through wire fraud.

21. Bank records reveal that the bank accounts were opened with a valid Illinois Secretary of State Identification Card number. According to Illinois Secretary of State records, the Identification Card number provided to the bank matches the Secretary of State records for ZHU. I have reviewed video surveillance and still photo images of the person who makes withdrawals from ZHU's Sea Dragon Trading and Sea Dragon Remodel accounts at JPMC and BOA, and this appears to be the same person depicted on ZHU's Illinois state identification card. In the bank surveillance videos, ZHU is seen making withdrawals inside branches. In each instance, ZHU was accompanied by Individual 1.[4]

[4] Law enforcement has identified Individual 1's real name; however, I will refer to him as Individual 1 to protect the privacy of an uncharged person.

22. ZHU is a Chinese citizen, who entered the United States on a tourism visa in January 2019 and has remained here ever since. From in and around September 2022, through in and around January 2023, ZHU's known financial and business activity occurred in the Southern California area. In January 2023, he traveled on a one-way plane ticket to Illinois. Law enforcement conducted a search of open-source corporate registries and did not locate any companies registered by ZHU in Illinois.

C. HAILONG ZHU's Bank Accounts Activity Establishes His Role in a Money Laundering Conspiracy

23. A review of the JPMC accounts ending in 5581 and 3886, which are in the names of Sea Dragon Remodeling and Sea Dragon Trading and were identified above, respectively, revealed that they were primarily funded by incoming wires sent by individuals located across the United States. These individuals appear to have no known reason for sending money to a remodeling or trading company located in Southern California. Moreover, the incoming wires were then immediately used to fund outgoing wires sent primarily to accounts in Hong Kong or at a known bank ("Bank 1") with offices in the United States. While this investigation is ongoing, thus far, law enforcement has identified that many of the remitters of the incoming wires to ZHU's Sea Dragon Trading and Sea Dragon Remodeling business bank accounts are victims of cryptocurrency investment frauds, or "Pig Butchering" scams.

24. Included among those victims who wired funds related to a cryptocurrency scam into ZHU's accounts, is an individual living in Falls Church, Virginia (hereinafter, "Victim 1"), an individual living in Santa Ana, California (hereinafter, "Victim 2"), and an individual living in Waldwick, New Jersey (hereinafter, "Victim 3").

25. However, there are many more suspected victims and law enforcement is working diligently to identify, notify, and interview these victims. In total, I estimate that there are

approximately 60 suspected victims associated with 60 wires to five bank accounts at three different banks, all in the names of Sea Dragon Trading or Sea Dragon Remodel. The suspected 60 wires are worth approximately $1.7 million in suspected fraudulent transfers.

a. Victim 1 Transfers

26. On or about January 6, 2022, law enforcement interviewed Victim 1. Victim 1 stated that in or around June 2022, they received an unsolicited call from a female, believed to be of Asian nationality. The female identified herself as "RACHELL" and stated that she lived in Miami, Florida. According to Victim 1, their initial conversation started with "RACHELL" apologizing for dialing the wrong number but quickly transitioned into a more inquisitive and general conversation. "RACHELL" provided Victim 1 with her Telegram handle, @rachel12587, and the conversation quickly transitioned to Telegram.[5]

27. Victim 1 stated that over the course of months the conversations became more "romantic" and eventually "RACHELL" introduced cryptocurrency investment ideas into the conversation. According to Victim 1, "RACHELL" eventually promoted a cryptocurrency investment domain named "coinasx.com," which appears to be a fraudulent cryptocurrency investment website that is spoofing the Australian Securities Exchange. Victim 1 visited the URL and downloaded an application associated with the platform onto their mobile device. The downloaded mobile platform uses the name "ASX," mimicking the Australian Securities Exchange.

28. "RACHELL" then encouraged Victim 1 to start investing and to request payment instructions from "ASX" online customer service. Victim 1, who is generally not comfortable with technology, did not set up an account with a cryptocurrency exchange, as originally requested by

[5] Telegram is an encrypted messaging service that also offers audio and video calling and file sharing.

the platform's customer service representatives. As a result, the customer service center encouraged Victim 1 to send wire transfers in lieu of cryptocurrency to make purported investments on "ASX."

29. On or about August 12, 2022, and after Victim 1 was provided with wire instructions from an "ASX" online customer service representative, Victim 1 made a $1,100 investment from their M&T bank account in Falls Church. Victim 1 then began seeing significant profits in their account and invested an additional $40,000 through wires between August and November 2022. Victim 1 initiated these wires from Falls Church, Virginia. I discussed the wire process with Bank of America and learned that the data associated with wires executed at a bank branch are captured and originate at that branch. From there, the data and instructions were sent to Bank of America data centers. As discussed below, I have confirmed that at least one of the wires was routed from the Bank of America branch in Falls Church, within the Eastern District of Virginia, to a data center in Levittown, Pennsylvania.

30. "ASX" customer service provided Victim 1 with different addresses for each wire transaction. Included in Victim 1's wire investments to the "ASX" cryptocurrency investment platform was a $5,000 wire on November 17, 2022, to BOA account 9529 belonging to Sea Dragon Remodel Inc., for which ZHU is the sole signatory. The wire instructions were provided by "ASX" online customer service and Victim 1 executed the wire on November 17, 2022, from their Bank of America account. Moreover, the Bank of America branch where Victim 1 executed the wire was in Falls Church, Virginia. Victim 1 was instructed to put "other" for the purpose of wire payment form. According to Bank of America, the wire on November 17, 2022, was sent from Falls Church, within the Eastern District of Virginia to a data center in Pennsylvania. Thus, the conspirators caused to be transmitted by means of wire communication in interstate commerce the

signs, signals, and writings described herein: the wire transfer sent on November 17, 2022, which was induced through fraud, from Victim 1, which was sent from within the Eastern District of Virginia to a data center in Pennsylvania.

31. Victim 1 informed law enforcement that they have been unable to make any withdrawals or recover any amount of their investments. Further, Victim 1 shared chat communications with law enforcement, and these messages corroborate Victim 1's statements.

b. Victim 2 Transfers

32. On January 9, 2023, law enforcement interviewed Victim 2. According to Victim 2, on or about September 2, 2022, they received a "wrong number" phone call from a named co-conspirator ("Co-Conspirator 1"). Co-Conspirator 1 informed Victim 2 that she was from Los Angeles and asked if they were interested in talking about cryptocurrency investments. Victim 2 and Co-Conspirator 1 then began speaking on Telegram. Victim 2 stated they deleted their communications with Co-Conspirator 1's Telegram account and could not remember the handle name for Co-Conspirator 1. Victim 2 noted that they believed their relationship to be a friendship and they spoke about cryptocurrency investments. Victim 2 informed law enforcement that around September 2022, Co-Conspirator 1 promoted a domain name "bitkancoin.com" ("BITKAN") to make cryptocurrency investments and showed Victim 2 how to set up an account.

33. On or about September 21, 2022, at Co-Conspirator 1's direction, Victim 2 made their first BITKAN "investment." Co-Conspirator 1 induced Victim 2 to invest by informing Victim 2 that they would receive a substantial return on their financial investment. Co-Conspirator 1 provided Victim 2 with wire instructions on Telegram and Victim 2 wired $3,000 from their Lakeland Bank account. Victim 2 noted they began to see a profit on their BITKAN account, and that Co-Conspirator 1 advised Victim 2 to continue making investments. Victim 2 noted that Co-

Conspirator 1 instructed them to consult the online customer service portal of BITKAN to make the next investment.

34. On or about November 2, 2022, Victim 2 received wire instructions from BITKAN online customer support and wired $20,000 from their Lakeland Bank account to the JPMC account 5581 belonging to Sea Dragon Remodel Inc. As stated above, ZHU is the sole signatory on this account. Shortly thereafter, Victim 2 attempted to withdraw their investments and was informed by someone purporting to work at BITKAN that an additional $86,000 investment was required to access Victim 2's funds. Victim 2 informed law enforcement that they discussed the situation with their financial advisor, which led Victim 2 to discover that they were scammed. Victim 2 has been unable to withdraw or recover any of their investment.

c. Victim 3 Transfers

35. On December 19, 2022, law enforcement interviewed Victim 3, who stated that they were a victim of a cryptocurrency investment scam. More specifically, Victim 3 invested $84,460 via wire transfers from their Bank of America account in a website called "gammaex.net" ("GAMMAEX"). Victim 3 noted that on or about August 24, 2022, they met an individual named "DANIEL" on a Facebook dating app and they began chatting on WhatsApp[6] and Telegram. Victim 3 noted that they believed they were in a romantic relationship with "DANIEL."

36. Victim 3 noted that "DANIEL" soon began promoting cryptocurrency investments and told Victim 3 they "can make a lot of money." According to Victim 3, Victim 3 did not understand cryptocurrency and "DANIEL" provided Victim 3 with a link to the GAMMAEX cryptocurrency investment website to start making investments. Victim 3 further stated that "DANIEL" instructed them to consult the online customer service portal to start making payments.

[6] Whatsapp is an encrypted messaging service that also offers audio and video calling and file sharing.

37. On or about September 26, 2022, Victim 3 sent $25,000 via wire from their Bank of America account to a wire address provided by the GAMMAEX customer service platform. Victim 3 then began to see significant profit and was encouraged to make additional investments. On or about October 12, 2022, Victim 3 wired another $31,000 from their Bank of America account to the JPMC account 3886 in the name of Sea Dragon Trading LLC. ZHU is the sole signatory of this bank account.

38. On or about October 24, 2022, Victim 3 then attempted to make a withdrawal from GAMMAEX but was told they could not until they paid additional taxes. On or about November 12, 2022, when unable to withdraw any investment proceeds, Victim 3 concluded that they had been a victim of a scam and ceased making additional investments.

39. Victim 3 has been unable to recover any of their investments. Victim 3 shared chat communications, which corroborate Victim 3's story and include the false and fraudulent statements that induced Victim 3 to invest in the scheme.

D. Sea Dragon Bank Account Transactions

40. Many of the wires observed going into ZHU's various bank accounts, including the wires mentioned above, came from individuals from across the United States with no known business or economic purpose. While most wires did not include a purpose or stated "other," in the section of the wire transfer form requesting "purpose of wire," others listed purposes that did not match with the description of ZHU's purported companies. For example, an incoming wire to one of ZHU's Bank of America accounts is reported to be for "home renovations," which would fit with the business of Sea Dragon Remodeling. However, the remitter of this wire lives in Maryland, not California, where Sea Dragon Remodeling is located. Furthermore, law enforcement searched a California Database of licensed contractors for Sea Dragon Remodel, Sea

Dragon Trading, and ZHU and found no results. Additionally, another wire sent to a Sea Dragon Remodel account was purportedly for "buying gold," which does not fit with any of the stated business purposes of Sea Dragon Remodel or Sea Dragon Trading.

41. ZHU was also found to have listed a different address for his businesses on different bank accounts that he opened. For example, for the JPMC account ending in 5581, opened in October 2022 under Sea Dragon Remodel, ZHU listed the business address as 4461 District Blvd, Vernon, California. This matches with the business records filed in October 2022 with the state of California for Sea Dragon Remodel Inc. However, Bank of America records reveal that on the Bank of America account ending in 9529, which was also opened in October 2022 for Sea Dragon Remodel Inc, ZHU listed the address as 2220 Falling Leaf Ave, Rosemead, California. Based on my training and experience, I know this is not a normal practice for legitimate businesses and is a known tactic used by criminals to conceal their identity and nature of their business.

42. According to bank records associated with ZHU's accounts, many of the incoming wires and cash deposits were used to fund outgoing international wires remitted shortly after money was sent in. For example, bank records show that between November 23 and 28, 2022, six wires were credited into ZHU's BOA account 9529, totaling $51,909.55. Included in these wires is the $5,000 wire that came in from Victim 1, who was located in Falls Church, Virginia, and other domestic wires from individuals with no apparent business reason. Shortly thereafter, on or about November 28, 2022, ZHU sent one wire for $53,000 to an account at a known bank ("Bank 2") in Nassau, Bahamas. Additionally, between October 21 and 24, 2022, JPMC account 3886 received $153,775 in three separate wires from unknown individuals. Again, ZHU is the sole signatory on this account. Then, on or about October 25, 2022, ZHU wired $152,000 to O

Diamonds Trading Limited, a company in Hong Kong.[7]

43. Further, law enforcement has not identified any purchases that can be associated with a home remodeling or trading company in ZHU's various bank accounts. Additionally, credit card activity seen on the Bank of America credit card ending in 6408 (which is linked to BOA account 3881), which is in Sea Dragon Trading's name, show charges at the Venetian Resort ("The Venetian"), a hotel and casino in Las Vegas, Nevada, and at a Louis Vuitton store, which are not business-related expenditures.

44. In addition, video surveillance provided by JPMC related to JPMC account 3886 and 5581 reveals unknown individuals making cash deposits into ZHU's Sea Dragon Trading and Sea Dragon Remodeling accounts. For example, on or about October 12, 2022, an unknown individual entered a JPMC branch in Brooklyn, New York to make a $15,000 deposit into JPMC account 3886 (Sea Dragon Trading). Additionally, on November 7, 2022, an unknown Asian female entered a JPMC branch in Houston, Texas to make an $18,000 deposit into JPMC account 5581 (Sea Dragon Remodel Inc). Based on my training and experience, I know it is highly unusual that individuals with no affiliation to a business would make a deposit on behalf of that business. Additionally, Sea Dragon Remodel and Sea Dragon Trading are reportedly a "Remodeling" and "Trading" company in California, so the transactions are even more suspicious because these deposits were made in Texas and New York. Based on my training and experience, I know that it is common for criminals laundering proceeds to request victims to make direct deposits into their

[7] As will be discussed in more detail below, I believe that ZHU maintained control of his accounts and executed these transfers. Not only is he the sole signatory on his accounts, but he was observed on video surveillance conducting transactions inside bank branches (Refer to section E "Video Surveillance Footage and Other Evidence Linking ZHU to Wire Transfers Made From His Bank Accounts" below) and JPMC and BOA records reveal that he accessed the bank statements to execute online wires using the phone number listed on his bank accounts (Refer to section E "Video Surveillance Footage and Other Evidence Linking ZHU to Wire Transfers Made From His Bank Accounts" below).

bank accounts.

45. Further review of financial records found mostly whole number wires (*e.g.* $100,000 and $75,000) coming in from remitters throughout the United States, including Massachusetts, Florida, Maryland, Illinois, Rhode Island, Kansas, Connecticut, New Jersey, Pennsylvania, South Dakota, Nebraska, Montana, and Louisiana, as well as one from Canada. It is highly unusual for a "Remodeling" or "Trading" company based in California to receive wires from customers out of state or in whole numbers.

E. Video Surveillance Footage and Other Evidence Linking ZHU to Wire Transfers Made From His Bank Accounts

46. Bank records, video surveillance footage, IP address information, and other evidence support that ZHU controls the bank accounts used to launder proceeds of wire fraud. Video surveillance obtained from JPMC and Bank of America confirm that ZHU was the individual executing outgoing wires to Hong Kong and other accounts. Specifically, JPMC and BOA video surveillance footage shows ZHU frequently using his phone while providing the tellers wiring instructions (Refer to Figure 2 below). As discussed above, in each instance for which video surveillance was available, ZHU was seen with Individual 1. Individual 1 stood behind ZHU during the transaction and his role is unknown.[8] Additionally, according to records provided by The Venetian, Individual 1 also accompanied ZHU to The Venetian.

47. According to records provided by The Venetian, ZHU provided his address on S El

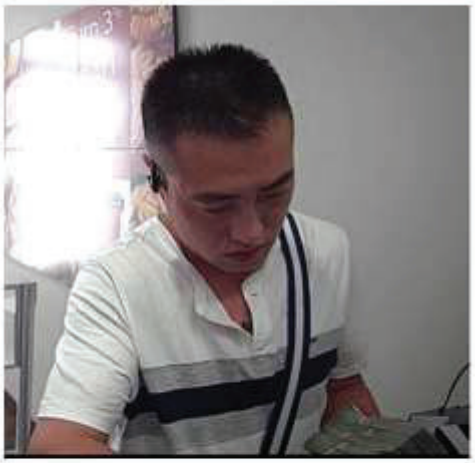
[8] On February 6 and 7, 2023, USSS agents conducted a surveillance operation of Individual 1. Over the two days, Individual 1 picked up three different individuals and drove them to five different bank branches. In each of these instances, Individual 1 entered the bank with the subjects just as he had done with ZHU in the bank surveillance video. On several occasions Individual 1 was seen holding documents and talking/using a cellular telephone. Based on my training and experience, I know that it is not normal behavior to frequent so many banks in one day. Individual 1's behavior of driving and accompanying numerous individuals to banks, and in some cases, the same bank but different locations, is an indication of potential money laundering.

Molino Street on numerous hotel invoices as recently as December 2022. Additionally, records pertaining to a credit check that was run by The Venetian also lists ZHU's address on S El Molino Street. According to Venetian records, ZHU deposited over $275,000 in cash from October to December 2022, which was during the time that the Pig Butchering scheme was ongoing. Law enforcement did not identify large cash withdrawals from ZHU's known bank accounts; thus, it is unclear how the cash deposited at The Venetian was obtained. Nonetheless, it is not a common business practice of legitimate "Remodeling and Trading" companies to receive bulk cash. Based on my training and experience, I know that money launderers use casinos to "wash" and launder fraudulently obtained bulk cash.

48. The images in Figure 2 below are still shots from video surveillance provide by JPMC and BOA. The first image shows ZHU with an earpiece in his ear and looking at his phone while executing a $6,000 cash withdrawal from his JPMC account 3886 (which is registered to an address associated with ZHU) at a JPMC branch in Arcadia, California (located approximately seven miles from an address known to be associate with ZHU). Based on my review of other video surveillance, I can say that ZHU is often wearing an earpiece and looking at his phone while executing wire transactions from bank locations. The second image is a still shot from a Bank of America branch located in Monterey Park, California, on October 28, 2022. This branch is located approximately two miles from an address associated with ZHU. In the still shot, ZHU is depositing $2,800 in cash into a Bank of America account in his name.

Figure 2

ZHU at JPMC branch (JPMC account 3886)



ZHU at BOA branch (BOA account 6689)

49. As referenced above, ZHU's listed phone number is phone number 1546 on both his business and individual bank accounts. JPMC records indicate online logins from an iPhone named "hailongiPhone" on both ZHU's Sea Dragon Trading and Sea Dragon Remodeling accounts using Verizon IP addresses geolocated to the Los Angeles area. Verizon records indicate that Verizon is the provider for phone number 1546. Verizon records further indicate that on November 23, 2022, phone number 1546 used Verizon IP address 174.195.197.26 and JPMC records reveal ZHU, using his mobile device named "hailongiPhone," attempted to log into JPMC account 3886 (Sea Dragon Trading) using the same IP address. JPMC records indicate that JPMC had already closed JPMC account 3886 due to fraud, therefore logging a "Failed" login attempt. Based on my training and experience, I know that an individual connecting to multiple online platforms utilizing the same IP address is using the same device. Considering that the device name is "hailongiPhone" and the user logs are to access bank accounts where ZHU is the sole signatory, I believe this indicates that ZHU is executing the online transactions and operating phone number 1546. JPMC records reveal ZHU logging into his online banking accounts to

conduct virtually all online banking activities from his ”hailongiPhone” iPhone device utilizing a Verizon IP address.

50. In addition, BOA records reveal online logins utilizing Verizon IP addresses, which match the JPMC online logins. For example, on or about November 10, 2022, JPMC account 5581 and BOA account 3881 were both accessed from IP address 174.193.200.48.

51. Verizon records reveal the subscriber for phone number 1546 to be Individual 2 with a listed Post Office box address in San Gabriel, California, which is close to ZHU's associated address in Alhambra, California.[9] Individual 2 also has a Wells Fargo bank account that lists the same address that ZHU listed on a bank account, which is an address located on S El Molino St in Alhambra, California. According to Verizon records, the phone was activated in September 2022, which is around the same time that the Sea Dragon entities and bank accounts were created and opened.

F. Attempted Obfuscation of International Wire Destinations as Evidence of ZHU's Money Laundering Activity

52. The way ZHU remitted funds to accounts held by Bank 2 shows an attempt to obscure the final destination of these funds. First, ZHU remitted the funds to Bank 1, a bank with a location in New York, by utilizing the JPMC correspondent account number at Bank 1. Bank records show that in the additional instructions section on the wire form, ZHU then instructed these wires were to be further credited to "xxxx0328." Further investigation reveals that that xxxx0328 was Bank 2's custody account at Bank 1. ZHU then listed in the additional instructions "DBT FFC xxxx179 00." Further investigation reveals that FFC means "For Further Credit," and xxxx179 00 is an account at Bank 2.

[9] Law enforcement has identified Individual 2's real name; however, I will refer to them as Individual 2 to protect the privacy of an uncharged person.

53. ZHU categorized these wires as domestic wires, indicating that they were being sent to an account at Bank 1 and marked on the wiring form that the country to which the wire was being sent was the United States. The wire form asks, "Will the further instructions provided result in the wire transfers being sent to an international bank or location?" to which ZHU answers "No." The use of the JPMC correspondent bank account and additional instructions show that ZHU is intentionally concealing the ultimate international destination of the proceeds by completing a wire form and adding "For Further Credit" details, which when followed will result in proceeds being in custody of Bank 2 in the Bahamas. Thus, ZHU knowingly took steps to transfer the funds to the Bahamas despite indicating that the funds would not be sent to an international bank or location.

54. Based on my training and experience, I know there is no legitimate purpose to structure a wire in this way. Moreover, the JPMC correspondent bank account and Bahamas bank custody account are considered propriety information and the bank restricts knowledge of the respective correspondent bank accounts for both domestic and foreign accounts to bank employees. Further, I know that international wires receive more scrutiny and take longer to process. As such, due to the increased risk of a fraudulent wire being called back by the bank, criminals prefer to use U.S. Bank accounts. JPMC and BOA records reveal that between October and December 2022, ZHU structured 18 wires totaling $1.1 million using the "for further credit" process described above to obfuscate funds going to the custody of a Bank 2 bank customer.

G. Evidence that ZHU Knew or was Willfully Blind to the Fact that the Bank Accounts Contained Proceeds Derived from Criminal Activity

55. Critically, the evidence reveals that ZHU knew that the proceeds were the result of illegal activity or that he was willfully blind to this fact. Between September 2022 and January 2023, ZHU opened at least seven different bank accounts at four different banks, of which at least five accounts have been closed by the banks due to fraud. ZHU was the sole signatory on each of

these accounts. Further, ZHU opened some of these accounts and continued to receive and send wires after at least some of the accounts were closed for fraud. In **Figure 3**[10] below, I convey the timeline of when accounts were opened and/or restricted.

Figure 3

Date	Bank Account	Entity	Status
9/9/2022	BOA account 3881	Sea Dragon Trading	Opened
9/9/2022	JPMC account 3886	Sea Dragon Trading	Opened
10/19/2022	BOA account 3881	Sea Dragon Trading	RESTRICTED due to Fraud
10/21/2022	BOA account 9529	Sea Dragon Remodel	Opened
10/21/2022	JPMC account 5581	Sea Dragon Remodel	Opened
10/27/2022	EWB account 4241	Sea Dragon Trading	Opened
10/28/2022	EWB account 4340	Sea Dragon Remodel	Opened
11/1/2022	WF account 6778	Sea Dragon Remodel	Opened
11/14/2022	JPMC account 3886	Sea Dragon Trading	RESTRICTED due to Fraud
11/14/2022	JPMC account 5581	Sea Dragon Remodel	RESTRICTED due to Fraud
12/8/2022	BOA account 9529	Sea Dragon Remodel	RESTRICTED due to Fraud
12/28/2022	BOA account 3881	Sea Dragon Trading	CLOSED for Fraud
1/3/2023	WF account 6778	Sea Dragon Remodel	CLOSED for Fraud

56. A Bank of America account was restricted due to fraudulent activity on October 19, 2022. Bank of America informed me that this account was restricted for fraud due to the numerous hold harmless requests that were filed on the account. Bank of America IP logs reveal that on October 24, 2022, ZHU attempted to login three times and was signed off due to suspected fraud on his account. The IP logs also reveal that on October 25, 2022, ZHU's account logged an event description named "ConvAsst:Customer_Inquiry:Status" indicating ZHU inquired online about his account status. Verizon IP logs on October 25, 2022, reveal ZHU utilized the Verizon phone number 1456 to access his Bank of America online portal. Additionally, Verizon records also reveal that Verizon phone number 1456 called Bank of America on October 25, 2023. On February 13, 2023, I learned from a Bank of America investigator that Bank of America will

[10] Figure 3 does not nor is it intended to represent all the accounts owned by ZHU. Further, the dates are approximate and were provided to me by bank investigators over the phone.

inform the customer when the customer attempts to access an account that has been restricted due to fraud. Therefore, since bank records reveal that ZHU made attempts to access his account, including calling Bank of America after his account was restricted due to the fraud, I believe he would have been informed of the suspected fraud.

57. On February 14, 2023, I spoke with a JPMC investigator and was informed that ZHU received an account restriction letter on his JPMC account on December 13, 2022. This letter, which I reviewed, informed ZHU that "Due to recent activity, or because we need more information from you, we have restricted your account, and it may close soon." The letter continues and informs ZHU, "please act quickly to better understand the restriction on your account – you may be able to provide information needed to keep your account open." The JPMC bank investigator informed me that on December 20, 2022, ZHU called to inquire about his account status. On this call, ZHU asked if his funds could be released and the banker informed ZHU that all funds in his account were held and would not be released. ZHU did not agree to provide additional information to the investigator who restricted his account. Based on my training and experience, I know that individuals with knowledge of a fraudulent transaction usually do not follow up with the bank investigator when questioned about a fraudulent transaction.

58. Further, bank records reveal that on December 19, 2022, a Wells Fargo bank investigator emailed ZHU at his listed gmail address informing him that his Wells Fargo account ending 6778 "was the beneficiary of funds in error and a referral to law enforcement has been made by the victim." The Wells Fargo investigator requested that ZHU arrange the "timely return" of funds and to discuss this matter with him to obtain additional details. The investigator informed ZHU that failure to respond may result in his account being restricted or closed. The email was sent from the investigator's Wells Fargo email account and his contact information was provided

for verification. The Wells Fargo account was closed on January 3, 2023. Further, ZHU never followed up with the bank. Based on my training and experience, I know that individuals with knowledge of a fraudulent transaction usually do not follow up with a bank investigator when questioned about a fraudulent transaction.

59. Additionally, bank records reveal that ZHU held a personal account at U.S. Bank ending 4148. On January 5, 2023, bank investigators spoke to ZHU on the phone to question him regarding suspicious activity seen on this account, in particular $187,000 in cash deposits and a $13,000 wire transfer from his personal East West Bank account ending in 9074. ZHU informed the bank investigators that he is based in Chicago, but that he works on construction projects in California for which his customers pay him in cash. Furthermore, U.S. Bank asked ZHU about the purpose of an attempted international wire transfer on December 1, 2022. ZHU responded that the payment was going to be for "construction/renovation materials to overseas suppliers."

60. As Figure 3 shows, after his Bank of America account was restricted on October 19, 2022, he continued to open accounts. Importantly, after the Bank of America and JPMC accounts were restricted or closed for fraud, ZHU continued to receive wires that were obtained from victims through a wire fraud scheme. For instance, Victim 1 located in Falls Church, Virginia, sent a wire induced through fraud on or about November 17, 2022, which is after Bank of America restricted the account for fraud. Indeed, JPMC moved to restrict accounts on November 14, 2022, which was three days prior to this wire. Despite Bank of America and JPMC account restrictions for fraud, ZHU continued to send wires overseas.

61. I submit there is probable cause to establish that ZHU knew that the proceeds wired into his account were obtained through criminal activity or that ZHU was willfully blind to this fact. The key evidence supporting this conclusion includes, but is not limited to: (1) the fact that

the bank accounts were set up for what is a shell entity with no business; (2) the pattern and amount of wires received; (3) ZHU's activity in sending wires overseas even though he indicated that the money was not being sent overseas in several instances; (4) the fact that ZHU's bank accounts were essentially pass through accounts for the wires and no business activity was being conducted; (5) the fact that Bank of America restricted the account ending in 3881 for fraud and ZHU continued to open accounts and send and receive wires; (6) the fact that ZHU continued to send wires after other bank accounts were restricted and/or closed in November and December; and (7) ZHU was made aware that his accounts were restricted due to fraud through restriction letters, his attempted login attempts, and actual conversations with bank officials.

CONCLUSION

62. Based on my knowledge, training, and experience, and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that, from at least September 2022 to the present, in the Eastern District of Virginia and elsewhere, the defendant, HAILONG ZHU, did knowingly and intentionally combine, conspire, confederate, and agree with others, both known and unknown, to commit an offense against the United States, in violation of Title 18, United States Code, Section 1956, to wit: to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of a specified unlawful activity, that is wire fraud, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of a specified unlawful activity, and that while conducting and attempting to conduct such financial transactions knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity in violation of Title 18, United States Code, Section 1956(a)(l)(B)(i), all in violation of Title 18, United States Code, Section 1956(h).

Christopher Saunders

Christopher Saunders
Special Agent
United States Secret Service

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this ____ day of March 2023.

Digitally signed by Ivan Davis
Date: 2023.03.10 12:30:34 -05'00'

The Honorable Ivan D. Davis
United States Magistrate Judge